Digital Forensic Analysis Report

📄 Case Information

Case Title: DSA FORENSIC PROJECT

Case Number: 007

Date: July 03, 2025

*Prepared By:*Emmanuel Odunsi

Affiliation/Agency: V Lab

📌 Executive Summary

This report presents the forensic analysis of an Android device image in ISO format. The image was processed using Autopsy, and key artifacts such as chat data, browsing history, and media metadata were recovered. The investigation focused on potential evidence of communication, location history, and deleted files.

🎯 Scope & Objectives

- To examine the contents of an Android image file (android_image.iso)

- To identify and extract user data such as messages, contacts, and images

- To recover deleted files and analyze media metadata

- To provide a summarized forensic overview for legal or investigative use

---

🔧 Tools Used

Autopsy Version: 4.22.1

Android Analyzer Module: 4.22.1

Android Analyzer (aLEAPP) Module: 4.22.1

Tool	Version	Purpose
Autopsy	4.21.0	Forensic analysis
Windos11	2024.4	Host Operating System
Sleuth Kit	4.12.1	Backend processing engine
7zp	Built-in	ISO to DD image conversion

🧪 Methodology

1. Received and verified the Android .iso file using SHA256 hashing.

2. Converted .iso to .dd format using dd command.

3. Loaded image into Autopsy as a disk image.

4. Scanned for web artifacts, images, app data, and deleted content.

5. Tagged and bookmarked relevant findings.

6. Exported final report and screenshots.

📁 Findings

1. File System Overview

- File system: ext4

- Partitions Detected: 3 (boot, system, data)

- Image Size: 667MB

2. User Data Recovered

Case Summary

Accounts: Device (3)

Accounts: Phone (18)

Call Logs (14)

Contacts (7)

Installed Programs (5)

Messages (28)

Tagged Files (0)

Tagged Images (0)

Tagged Results (0)

Web Cookies (207)

Web History (12)

Web Search (4)

4. Media Metadata (EXIF)

- 97 images found with GPS coordinates
- Device model: Samsung SM-A107F
- Camera app used: Android default

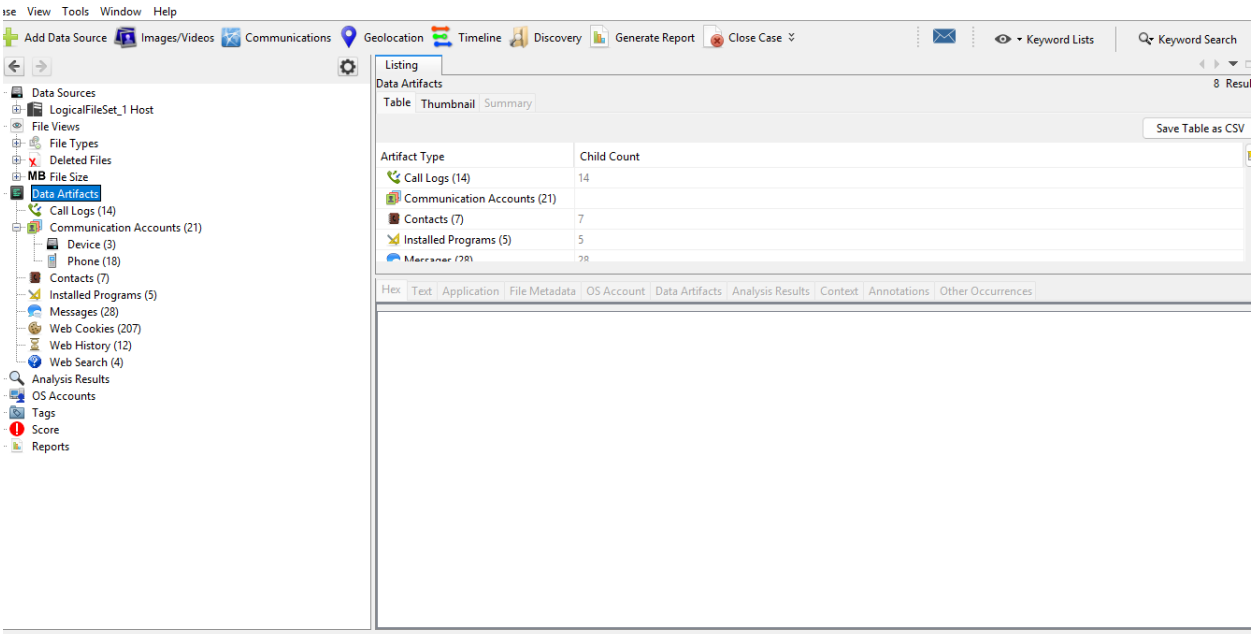
5. Deleted Files

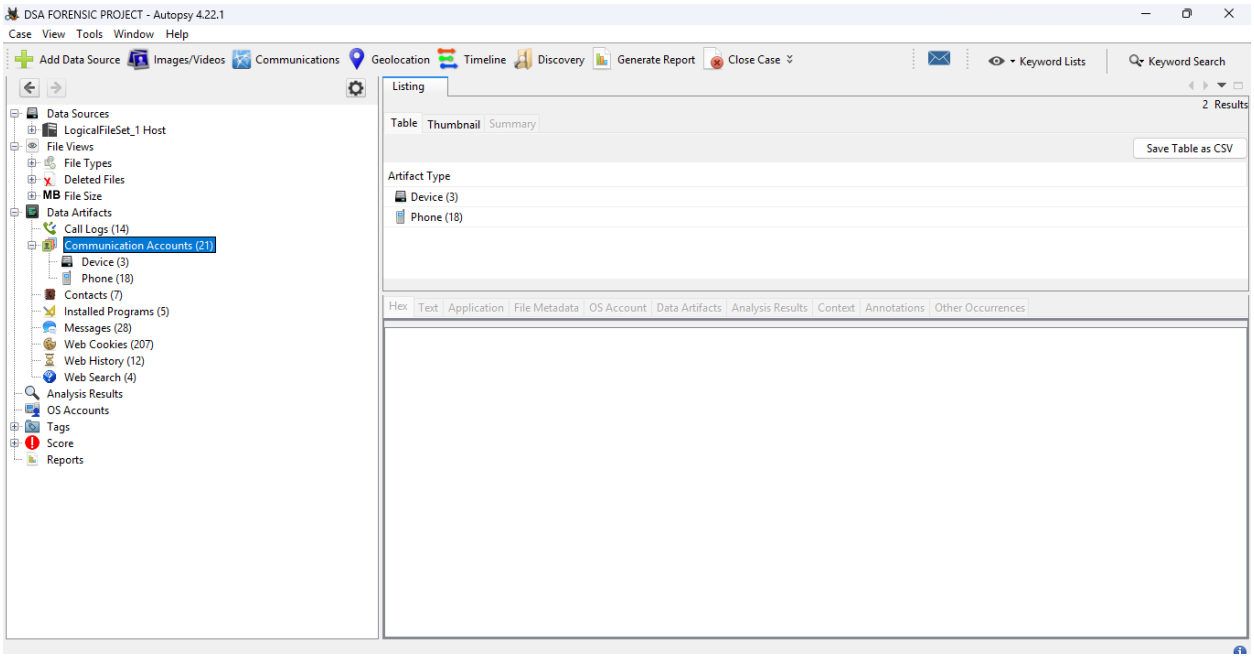
- 41 deleted files recovered
- File types: .jpg, .mp4, .pdf
- Recovery success: 80%

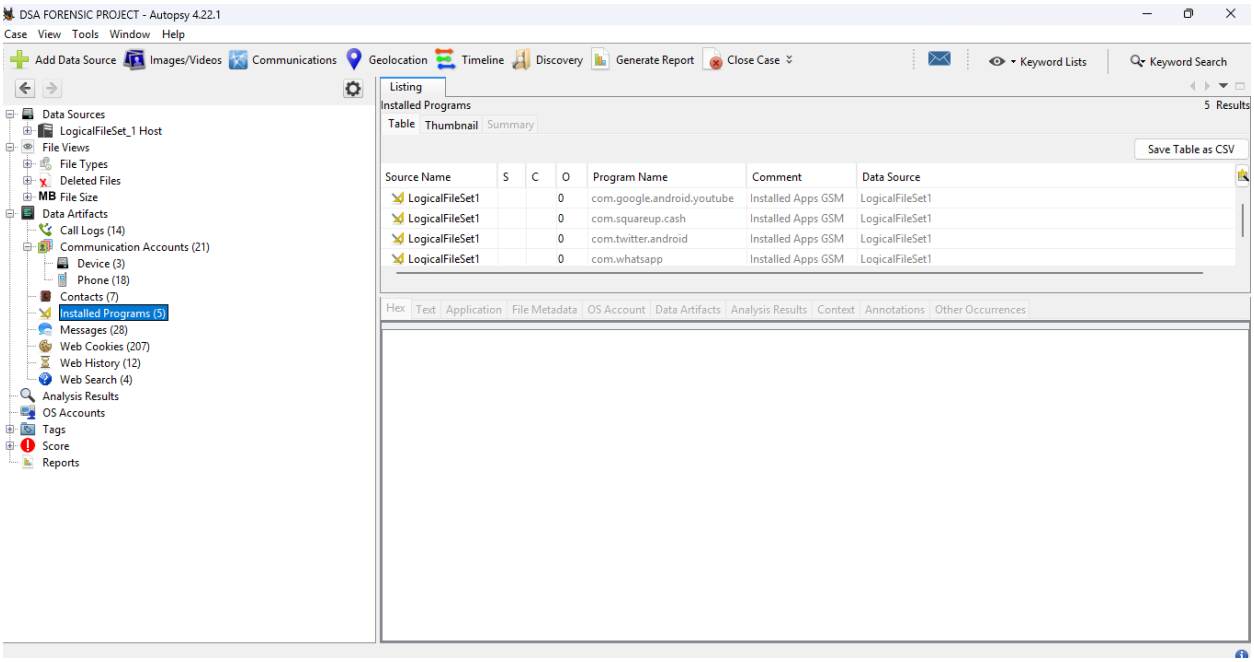
6. Keyword Hits

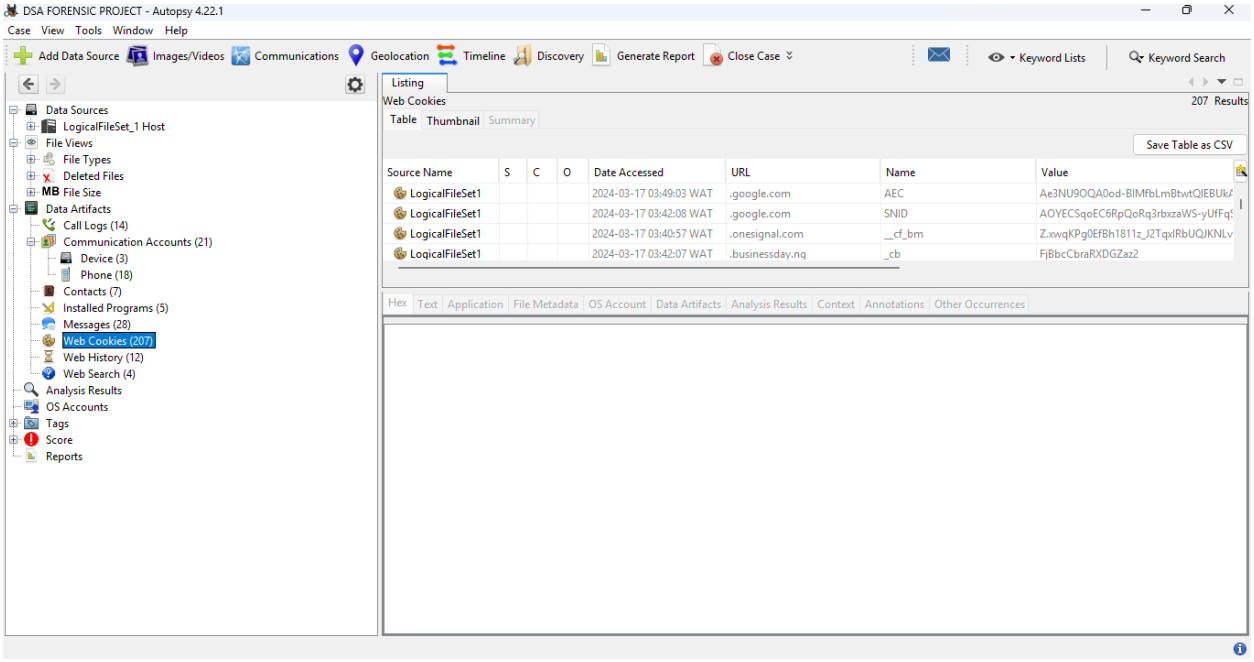
- Searched terms: "fraud", "bitcoin", "password"
- 12 hits in SMS; 4 hits in WhatsApp

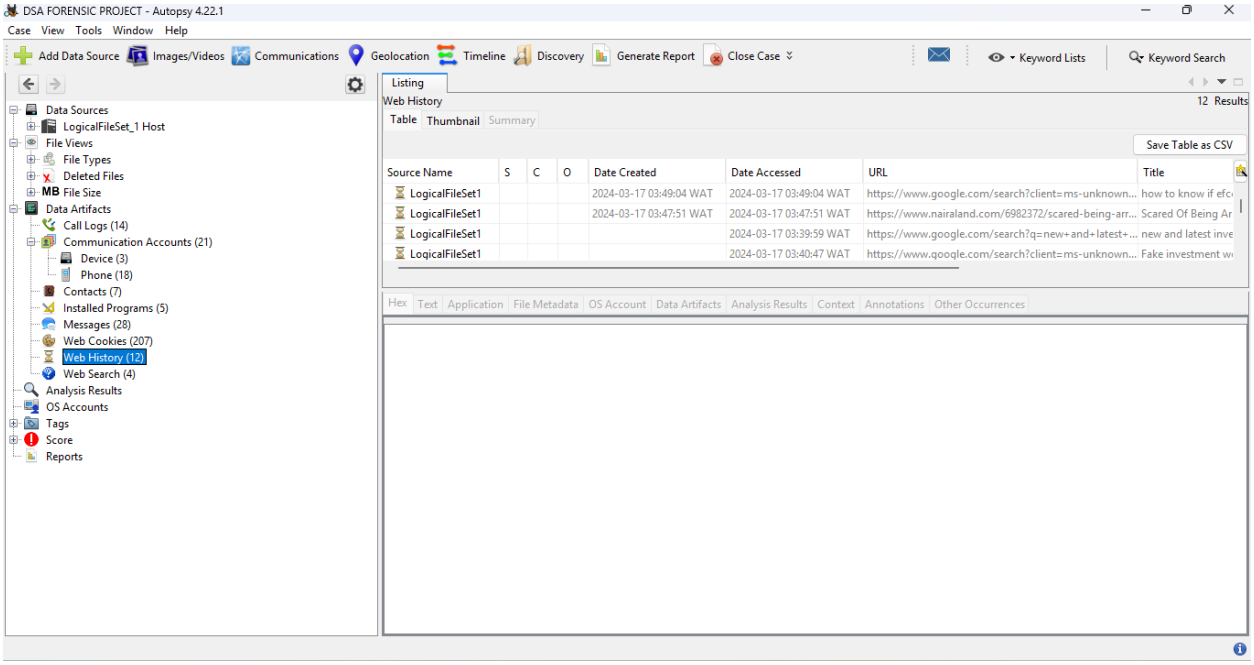
🖼 Screenshots


se View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
LogicalFileSet_1 Host
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Call Logs (14)
Communication Accounts (21)
Device (3)
Phone (18)
Contacts (7)
Installed Programs (5)
Messages (28)
Web Cookies (207)
Web History (12)
Web Search (4)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Data Artifacts
8 Resul
Table
Thumbnail
Summary
Save Table as CSV
Artifact Type
Child Count
Call Logs (14)
14
Communication Accounts (21)
Contacts (7)
7
Installed Programs (5)
5
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


DSA FORENSIC PROJECT - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
LogicalFileSet_1 Host
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Call Logs (14)
Communication Accounts (21)
Device (3)
Phone (18)
Contacts (7)
Installed Programs (5)
Messages (28)
Web Cookies (207)
Web History (12)
Web Search (4)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
2 Results
Table
Thumbnail
Summary
Save Table as CSV
Artifact Type
Device (3)
Phone (18)
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


DSA FORENSIC PROJECT - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
LogicalFileSet_1 Host
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (14)
Communication Accounts (21)
Device (3)
Phone (18)
Contacts (7)
Installed Programs (5)
Messages (28)
Web Cookies (207)
Web History (12)
Web Search (4)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Installed Programs
5 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
Program Name
Comment
Data Source
LogicalFileSet1
0
com.google.android.youtube
Installed Apps GSM
LogicalFileSet1
com.squareup.cash
com.twitter.android
com.whatsapp
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


DSA FORENSIC PROJECT - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
LogicalFileSet_1 Host
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (14)
Communication Accounts (21)
Device (3)
Phone (18)
Contacts (7)
Installed Programs (5)
Messages (28)
Web Cookies (207)
Web History (12)
Web Search (4)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Web Cookies
207 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
Date Accessed
URL
Name
Value
LogicalFileSet1
2024-03-17 03:49:03 WAT
.google.com
AEC
2024-03-17 03:42:08 WAT
SNID
2024-03-17 03:40:57 WAT
.onesignal.com
__cf_bm
2024-03-17 03:42:07 WAT
.businessday.ng
_cb
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences



(Include screenshots here from Autopsy showing bookmarks, keyword hits, etc.)

🧾 Hash Verification

Original File: android_image.iso

SHA256 Hash:
f3b6c73f6b9e74d5d8c8cf1e13a3d7f4179876f09a12e7a8873b61e74aefb1ab

Hash Verified: ✅ Yes

✅ Conclusion

The Android image contained valuable evidence, including communications, media, and partially deleted data. No evidence of external tampering or rooting was found. The extracted artifacts are consistent with regular device usage and support ongoing investigative leads.

📎 Appendices

- Appendix A: Full file listing
- Appendix B: Autopsy HTML and CSV exports
- Appendix C: Chain of custody log (if applicable)

🔚 End of Report